R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 24 JUIN 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

CERTIFIED COPY OF
PRIORITY DOCUMENT

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*02

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire — DB 540 @ W / 010801

Réservé à l'INPI

REMISE DES PIÈCES
DATE 18 NOV 2003
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0313507
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 18 NOV. 2003

Vos références pour ce dossier *(facultatif)* 35175/FR

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

BREESE-MAJEROWICZ
3 avenue de l'Opéra
75001 PARIS

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — **Cochez l'une des 4 cases suivantes**

Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

METHODE DE REDUCTION MODULAIRE ALEATOIRE ET EQUIPEMENT ASSOCIE

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) — ☒ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		Atmel Corporation
Prénoms		
Forme juridique		constituée selon les lois de l'État du Delaware
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	2325 Orchard Parkway
	Code postal et ville	SAN JOSE California 95131
	Pays	U.S.A.
Nationalité		U.S.A.
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 18 NOV 2003
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0313507

DB 540 @ W / 010801

Vos références pour ce dossier : *(facultatif)*		35175/FR
6 MANDATAIRE *(s'il y a lieu)*		
Nom		BREESE
Prénom		Pierre
Cabinet ou Société		BREESE-MAJEROWICZ
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	3 avenue de l'Opéra
	Code postal et ville	7 5 0 0 1 Paris
	Pays	France
N° de téléphone *(facultatif)*		01 47 03 67 77
N° de télécopie *(facultatif)*		01 47 03 67 78
Adresse électronique *(facultatif)*		office@breese.fr
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) BREESE Pierre 921038	**VISA DE LA PRÉFECTURE OU DE L'INPI** L. MARIELLO

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

METHODE DE REDUCTION MODULAIRE ALEATOIRE ET EQUIPEMENT ASSOCIE

La présente invention concerne une méthode de traitement et de calcul arithmétique, destinée à être utilisés particulièrement dans les applications cryptographiques. La présente invention concerne en particulier le calcul des résidus impliquant une réduction modulaire, particulièrement les calculs dérivés de la méthode de réduction de Barrett.

De nombreux algorithmes cryptographiques utilisent la multiplication (ou l'exponentiation) de grands entiers et la réduction du produit à une valeur résiduelle qui est congruente avec un module spécifié associé à la clé cryptographique. Ces calculs peuvent faire l'objet d'attaques d'horloge et d'analyses de puissance. Il est donc important que ces calculs soient sécurisés de sorte que les informations sur la clé ne puissent être obtenues.

En même temps, il est important que ces calculs soient rapides et précis. La multiplication et la réduction de grands entiers est généralement la partie exigeant le plus de calculs d'un algorithme cryptographique. Plusieurs techniques distinctes de calcul ont été développées en vue d'une réduction modulaire efficace, y compris celles connues sous le nom de méthode de Quisqueter, de méthode de Barrett et de méthode de Montgomery, et de modifications impliquant des calculs préliminaires et une consultation de table. Ces techniques bien connues sont décrites et comparées dans l'art antérieur. Voir, par exemple : (1) A. Bosselaers et al., « Comparison of three modular reduction functions », , Advances in Cryptology/Crypto '93, LNCS 773, Springer-

Verlag, 1994, pp. 175-186. (2) Jean-François Dhem, « Design of an efficient public key cryptographic library for RISC-based smart cards », thèse de doctorat, Université catholique de Louvain, Louvain-la-Neuve, Belgique, mai 1998. (3) C. H. Lim et al., « Fast Modular Reduction with Precomputation », publication préliminaire, 1999 (disponible à la CiteSeer Scientific Literature Digital Library, citeseer.nj.nec.com/109504.html). (4) Hollmann et al., « Method and Device for Executing a Decrypting Mechanism through Calculating a Standardized Modular Exponentiation for Thwarting Timing Attacks », brevet US n°6 366 673 B1, Apr. 2 2002 (basé sur la demande déposée le 15 septembre 1998).

Un objectif de la présente invention est d'améliorer la méthode de réduction modulaire de Barrett et le dispositif de calcul à cet effet, afin de le sécuriser davantage contre les attaques de cryptoanalyse, tout en continuant à obtenir des résultats rapides et précis.

Un autre objectif de la présente invention est de proposer la méthode améliorée susmentionnée et un dispositif qui accélère l'estimation de quotient.

Ces objets sont atteints par une méthode de réduction modulaire exécutée par ordinateur dans laquelle un quotient utilisé pour le calcul est systématiquement sous-estimé avec une erreur aléatoire de quelques bits, par exemple de moins d'un demi-mot. Le reste résultant est toujours congruent par rapport au produit intermédiaire correspondant associé au module spécifié, mais est plus grand que la valeur résiduelle et diffère de façon aléatoire d'une exécution à l'autre. Du fait que le quotient a seulement besoin d'être approximé, son estimation est plus rapide. Du fait que l'erreur

d'estimation est délibérément aléatoire, cette méthode est plus sûre pour la prévention contre la cryptoanalyse. Toutefois, les résultats intermédiaires sont mathématiquement équivalents (congruents par rapport aux résultats réels), et le résultat final (après un ensemble final de soustractions du module) est exactement le même, ce qui permet d'atteindre la précision nécessaire pour pouvoir inverser les opérations cryptographiques.

L'équipement utilisé pour exécuter les étapes de la méthode selon la présente invention comprend un générateur de nombres aléatoires pour injecter une erreur aléatoire dans l'estimation du quotient. Une unité de calcul à accès mémoire et injection de report opère sous contrôle d'un micrologiciel exécutant un séquenceur d'opérations pour exécuter les étapes de multiplication-accumulation au niveau mot nécessaires à la multiplication et à la réduction modulaire de grands entiers.

La figure 1 est une vue en plan schématique de l'équipement de calcul selon la présente invention (y compris un générateur de nombres aléatoires) utilisé pour exécuter la méthode de réduction modulaire selon la présente invention.

La figure 2 est un organigramme illustrant les étapes générales de la présente méthode de réduction modulaire.

Sur la figure 1, l'équipement de calcul comprend une unité de calcul 10 capable d'exécuter les étapes de multiplication au niveau mot et de multiplication-accumulation d'opérandes extraits à partir de la mémoire (RAM) 12 et de termes de report issus des registres 14. Le séquenceur d'opérations 16 comprend des circuits logiques pour contrôler l'unité de calcul 10 en accord avec les instructions de micrologiciel ou de logiciel pour exécuter

l'ensemble des opérations de multiplication (ou d'exponentiation) et la réduction modulaire de grands entiers. Les paramètres des opérations, stockés dans les registres 18 accessibles par le séquenceur d'opérations 16, consistent en pointeurs qui permettent au séquenceur d'opérations de situer un opérateur dans la RAM 12, ainsi que des informations sur la longueur (nombre de mots) des opérandes, les informations de contrôle d'injection de reports, et l'adresse de destination des résultats intermédiaires. Jusqu'à présent, ce dispositif est pratiquement similaire aux autres équipements adaptés aux opérations arithmétiques sur les grands entiers. En dehors des détails des étapes de réduction, qui seront décrits plus bas, les instructions de micrologiciel ou de logiciel sont également similaires aux programmes antérieurs pour l'exécution de multiplications ou d'exponentiations efficaces sur des grands entiers dans des segments de niveau mot.

A la différence des équipements antérieurs de ce type, l'équipement de la figure 1 comprend également un générateur de nombres aléatoires 20 qui, par exemple, peut être tout circuit générateur de nombres pseudo-aléatoires connu. Ce générateur de nombres aléatoires exécute un calcul et produit un nombre aléatoire utilisé dans la présente méthode. Ici le générateur de nombres aléatoires 20 est accédé par l'unité de calcul 10, sous commande du séquenceur d'opérations 16 en accord avec les instructions de programmes exécutant la méthode selon la présente invention, de façon à injecter la quantité d'erreur aléatoire dans l'estimation du quotient, comme décrit ci-dessous.

Sur la figure 2, la méthode selon la présente invention est une amélioration de la technique de réduction modulaire de Barrett, en exécutant une estimation de quotient plus rapide et en permettant de résister aux attaques de cryptoanalyse. Cette méthode est exécutée par l'équipement de la figure 1.

La réduction modulaire résout généralement

$R \equiv X \bmod M \equiv X - \lfloor X/M \rfloor M$, où R est la valeur résiduelle à déterminer qui est congruente avec X pour le module M, et le symbole $\lfloor a \rfloor$ représente la partie entière (le plus grand entier $\leq$ a) de telle sorte que $\lfloor X/M \rfloor$ correspond à une division d'entier. Le nombre X à réduire est typiquement un produit de deux grands entiers (généralement premiers), X = A.B, autrement dit l'un ou les deux parmi les entiers A et B ont une taille de plusieurs mots (ex. A et B peuvent être chacun de 1024 bits, ou 32 mots de 32 bits de long). Dans tous les cas, le problème de base dans toute méthode de réduction modulaire réside dans l'évaluation du quotient $q = \lfloor X/M \rfloor$ de manière efficace pour de grands nombres (multi-mots) X et M. Dans la présente invention, un problème supplémentaire réside dans l'exécution de la réduction d'une manière sécurisée contre les attaques d'analyse de puissance dans les applications cryptographiques.

La méthode de Barrett implique le calcul préliminaire et le stockage d'une estimation mise à l'échelle de la réciproque du module, U, et le remplacement de la longue division par des multiplications et des décalages de mots (division par b) afin d'estimer le quotient. Avec le choix approprié de paramètres, l'erreur d'estimation du quotient

est au plus de deux. La présente invention améliore la méthode de Barrett en effectuant seulement une approximation du quotient par une estimation moins précise mais plus rapide, et en injectant intentionnellement une erreur aléatoire dans le quotient avant de calculer le reste. Le reste résultant sera plus légèrement plus grand que, mais congruent avec, la valeur résiduelle.

Supposons que w représente la taille de mot (ex. w = 32 pour les processeurs 32 bits), $b = 2^w$ représente la racine, n est la longueur du module M en mots, où

$$M = \Sigma_{i=0}^{n-1} m_i b^i,$$
$$0 < m_{n-1} < b,$$
$$0 \leq m_i < b, \text{ pour } i = 0 \text{ à } n-2,$$
$$b^{n-1} \leq M < b^n,$$

et X est le nombre à réduire, qui a une longueur maximum de 2n +1 mots, c'est-à-dire que

$$X = \Sigma_{i=0}^{2n} x_i b^i,$$
$$0 \leq x_i < b, \text{ pour } i = 0 \text{ à } 2n,$$
$0 \leq X < b^{2n+1}$ (ou $M \leq X < b^{2n+1}$, dans certaines circonstances)

Nous commençons à calculer de façon préliminaire et à stocker (étape 30 de la figure 2) une constante U représentant la réciproque mise à l'échelle du module M

$$U = \lfloor b^{2n+1}/M \rfloor = \lfloor 2^{2nw+w}/M \rfloor$$

Cette valeur stockée est alors utilisée ensuite dans toutes les opérations de réduction de ce module particulier M. U a toujours une longueur de n+1 mots pour chaque module M qui n'est pas une puissance de b.

Pour exécuter une réduction de module de X, nous estimons un quotient q (étape 32) en utilisant la valeur stockée U,

$$q = \lfloor (\lfloor X/b^n \rfloor .U) /b^{n+2} \rfloor = \lfloor (\lfloor X/2^{nw} \rfloor .U) /2^{nw+2w} \rfloor$$

Ceci n'exige que des multiplications et des décalages de mots pour le calcul. Les parties entières tendent à garantir que le quotient q est toujours sous-estimé (jamais surestimé), bien qu'il soit possible que l'estimation du quotient se révèle être exacte. Une soustraction supplémentaire de un peut être incluse si une sous-estimation est nécessaire. Le quotient U et l'estimation du quotient diffèrent tous deux de celles de Barrett d'un décalage supplémentaire d'un mot chacun. (Barrett utilise $U = \lfloor b^{2n}/M \rfloor$ et $q = \lfloor (\lfloor X/b^{n-1} \rfloor .U) / b^{n+1} \rfloor$.) Le quotient estimé $q \geq 0$ aura une longueur maximum de n+1 mots.

A ce stade, il est préférable d'injecter (étape 36) une erreur aléatoire E dans le quotient calculé de façon à obtenir un quotient aléatoire, $q' = q - E$. Dans ce cas, nous devons avoir $M \cdot 2^{w/2} \leq X < b^{2n+1}$ pour éviter d'avoir des nombres négatifs. L'erreur aléatoire E peut être générée (étape 34) à partir de tout générateur de nombres aléatoires ou pseudo-aléatoires (matériel ou logiciel). La seule contrainte est que l'erreur soit dans une plage spécifiée, de telle sorte que

$$0 \leq E < (2^{w/2} - 1)$$

Ceci limite l'erreur potentielle introduite par le générateur aléatoire à un nombre de bits spécifié, ex. un demi-mot, en plus de toute erreur provenant de l'estimation du quotient elle-même.

Nous calculons ensuite (étape 38) le reste R' qui sera congruent (module M) avec la valeur résiduelle R :

$$R' = X - q'M$$

Du fait que le quotient q est sous-estimé, et qu'une erreur aléatoire E est introduite, le reste $R' \geq R$, à savoir le reste calculé, sera supérieur ou égal au résidu d'un petit multiple aléatoire du module M.

Le reste aléatoire R' peut être utilisé dans des calculs ultérieurs (étape 48), du type multiplication ou addition, avec un autre reste R'' (aléatoire ou non) qui, si nécessaire, est encore réduit (en revenant à l'étape 32) pour la cohérence. (L'erreur reste limitée).

En variante, si un résultat aléatoire n'est pas requis, nous pouvons choisir de conserver le quotient rapproché q (étape 44). Dans ce cas, nous pouvons avoir $0 \leq X \leq b^{2n+1}$. Le fait de conserver le quotient proche va permettre d'obtenir le vrai reste (étapes 46 et 40).

Finalement, en fonction des besoins de l'application particulière, le résidu R peut être calculé à partir du reste R' en appliquant des soustractions du module M (étape 40) jusqu'à ce que cette valeur soit inférieur à M. La valeur résiduelle R qui est égale à R' après la soustraction finale peut alors être renvoyée afin d'être utilisée dans le reste du système cryptographique (étape 42).

La randomisation de la réduction modulaire constitue une protection contre les diverses attaques de cryptoanalyse qui reposent sur la constance de l'utilisation des puissances pour déterminer le module.

Ici, la réduction de X modulo M varie de façon aléatoire d'une exécution à l'autre, tout en continuant à produire un reste intermédiaire R' qui est congruent. Le nombre de soustractions à la fin pour générer une valeur résiduelle finale R varie également de façon aléatoire d'une exécution à l'autre. Le nombre X à réduire de cette façon peut être obtenu à partir de diverses opérations mathématiques, y compris la multiplication, la mise au carré, l'exponentiation, l'addition, etc. De même, le module M à utiliser peut être dérivé de plusieurs manières, le plus souvent en cryptographie à partir d'une clé. La méthode de réduction modulaire aléatoire selon la présente invention est utile dans de nombreux algorithmes cryptographiques qui reposent sur cette réduction, dont les système cryptographiques à clé publique basés sur des grands premiers (par exemple RSA) et basés sur une courbe elliptique.

REVENDICATIONS

1 . Méthode de réduction modulaire exécutée par ordinateur sécurisée à des fins cryptographiques, comprenant :

le calcul préliminaire et le stockage en mémoire d'une constante U représentant une réciproque approximative au niveau bits d'un module M ;

l'estimation d'un quotient approximatif q pour un nombre X à réduire modulo M, dans lequel ladite estimation est exécutée sur X dans une unité de calcul, par multiplication par ladite constante U et par décalages de bits de X et par décalage de ladite multiplication ;

la génération dans un générateur de nombres aléatoires d'une valeur d'erreur aléatoire E et l'application de ladite valeur d'erreur audit quotient approximatif pour obtenir un quotient aléatoire $q' = q - E$; et

le calcul d'un reste $R' = X - q'M$ dans ladite unité de calcul, ledit reste étant supérieur audit module M mais congruent avec X modulo M.

2 . Méthode selon la revendication 1 dans laquelle le calcul préliminaire de ladite constante U est exécuté selon l'équation $U = \lfloor b^{2n+1}/M \rfloor$, où $b = 2^w$, w étant la taille en mots de l'unité de calcul en bits.

3 . Méthode selon la revendication 2 dans laquelle l'estimation du quotient approximatif q est exécutée par l'unité de calcul selon l'équation $q = \lfloor (\lfloor X/b^n \rfloor . U) /b^{n+2} \rfloor$

4. Méthode selon la revendication 3 dans laquelle une soustraction supplémentaire de un est comprise dans l'estimation du quotient.

5. Méthode selon la revendication 1 dans laquelle la réduction modulaire de X fait partie d'un programme de cryptographie exécuté par ordinateur.

6. Méthode selon la revendication 1 dans laquelle un trajet de circulation alterné est assuré entre la génération et l'application d'une valeur d'erreur au quotient approximatif peut être omise de façon sélective.

7. Méthode selon la revendication 1 dans laquelle le générateur de nombres aléatoires a une limite d'erreur spécifiée d'un demi-mot, moyennant quoi $0 \leq E < (2^{w/2} - 1)$.

8. Equipement de calcul pour l'exécution d'une méthode de réduction modulaire sécurisée à des fins cryptographiques, cet équipement comprenant :

une unité de calcul adaptée pour exécuter des étapes de multiplication et d'accumulation au niveau mots sur des opérandes extraits de la mémoire et des termes de report issus d'un ensemble de registres ;

un générateur de nombres aléatoires pour générer une valeur d'erreur aléatoire E ;

un séquenceur d'opérations comprenant des circuits logiques pour contrôler l'unité de calcul, et un générateur de nombres aléatoires en accord avec des instructions de programme afin d'exécuter la réduction modulaire d'un nombre X par rapport à un module M, ce qui implique au moins une estimation d'un quotient

approximatif q à partir d'une constante stockée au préalable U représentant une réciproque approximative en bits du module, une randomisation dudit quotient approximatif avec ladite valeur d'erreur E pour obtenir un quotient aléatoire $q' = q - E$, et un calcul d'une valeur de reste $R' - X - q'M$.

9. Equipement de calcul selon la revendication 8 comprenant en outre des registres de paramètres d'opérations accessibles par ledit séquenceur d'opérations, lesdits registres contenant un ou plusieurs parmi (a) des pointeurs pour situer l'opérande dans ladite mémoire, (b) des informations sur les longueurs des opérandes, (c) des informations de contrôle d'injection de report pour les registres de termes de report, et (d) des informations d'adresses de destination pour les résultats intermédiaires des étapes d'opérations.

10. Equipement de calcul selon la revendication 8 dans lequel la constante préstockée U dans ladite mémoire est obtenue par un calcul préliminaire selon l'équation $U = \lfloor b^{2n+1}/M \rfloor$, où $b = 2^w$, w étant la taille de mot de l'unité de calculs en bits.

11. Equipement de calcul selon la revendication 10 dans lequel l'estimation dudit quotient approximatif q exécutée par ladite unité de calcul sous contrôle dudit séquenceur d'opérations exécutant les exécutions de programme est effectuée selon l'équation $q = \lfloor (\lfloor X/b^n \rfloor . U) /b^{n+2} \rfloor$.

12. Equipement de calcul selon la revendication 11 dans lequel l'estimation de quotient exécutée par l'unité de calcul comprend une soustraction supplémentaire de un.

13. Equipement de calcul selon la revendication 8 dans lequel le générateur de nombres aléatoires a une limite d'erreur spécifiée d'un demi-mot, moyennant quoi $0 \leq E < (2^{w/2} - 1)$.

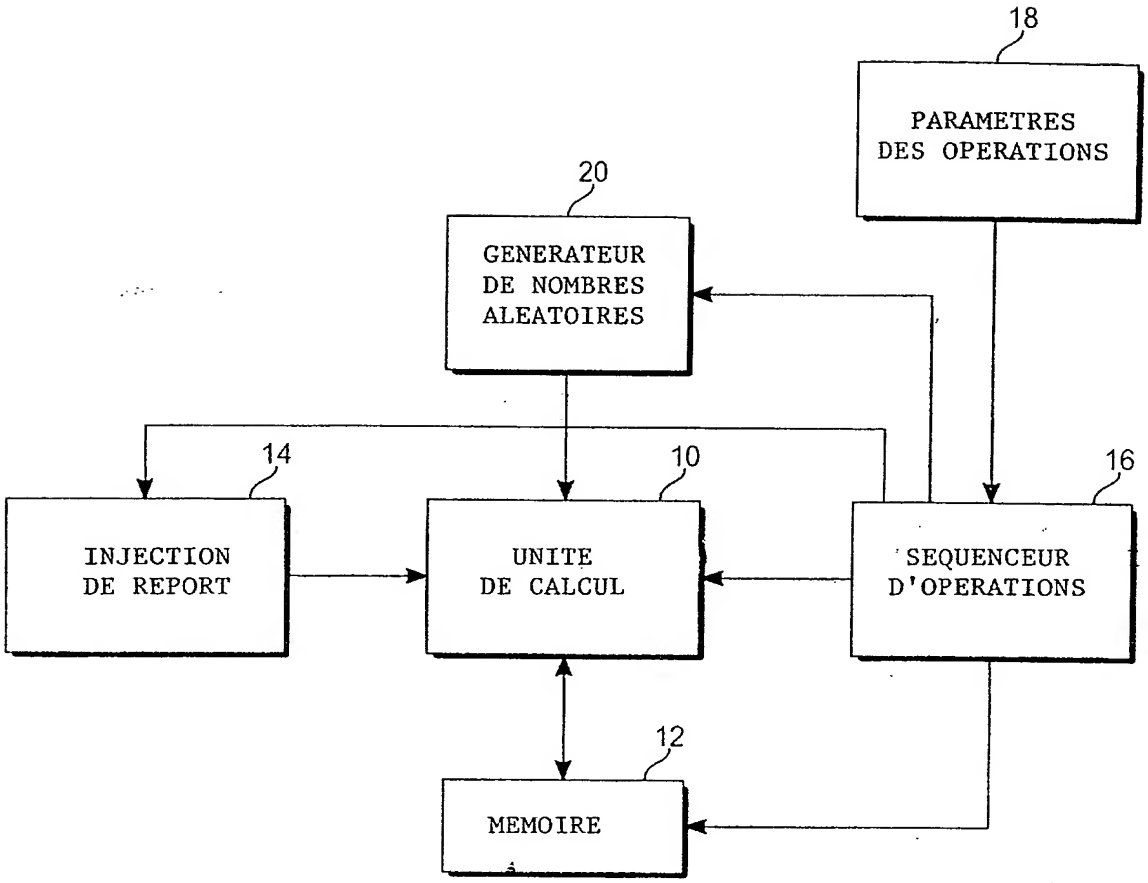
18
PARAMETRES
DES OPERATIONS
20
GENERATEUR
DE NOMBRES
ALEATOIRES
14
10
16
INJECTION
DE REPORT
UNITE
DE CALCUL
SEQUENCEUR
D'OPERATIONS
12
MEMOIRE

Fig._1

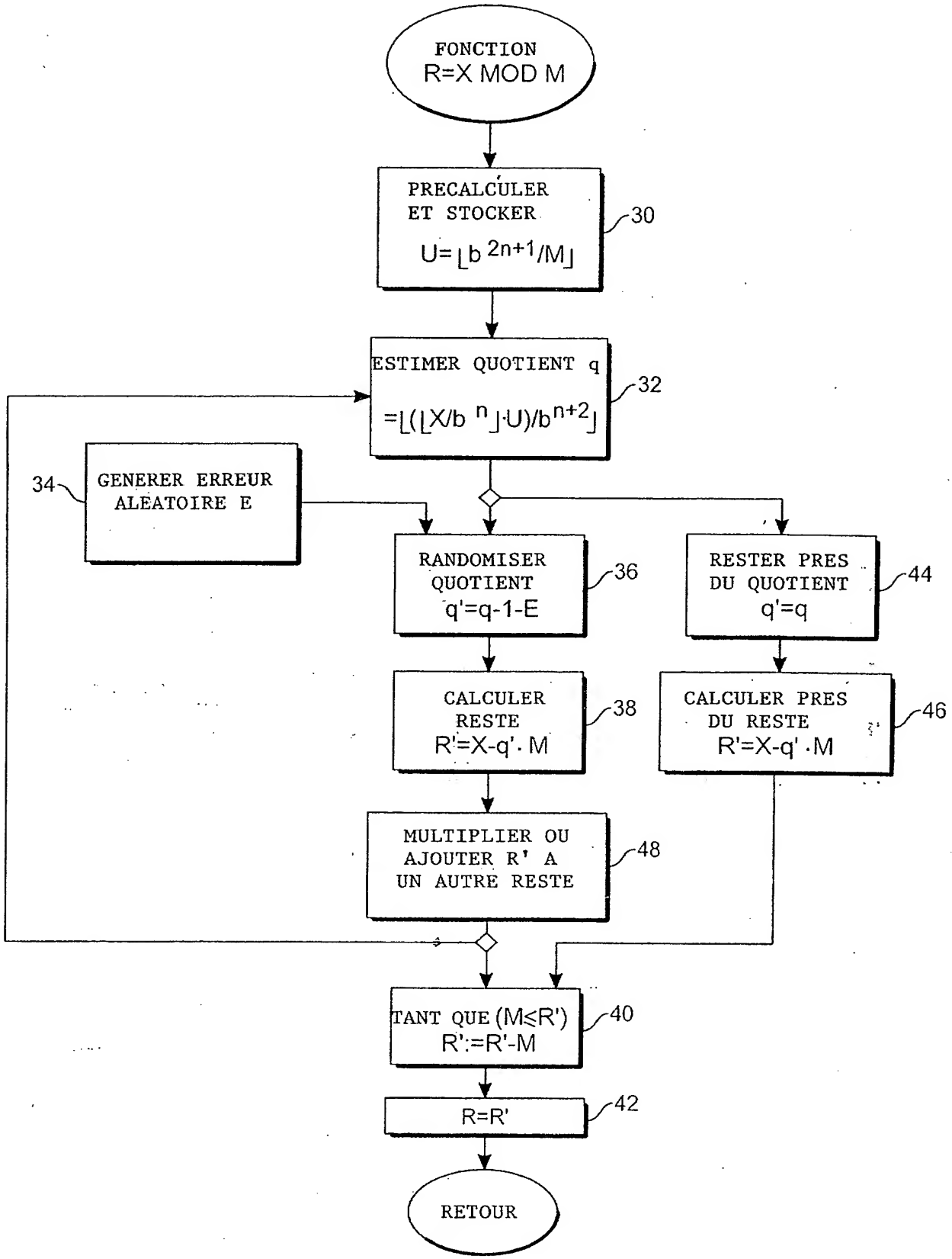
FONCTION
R=X MOD M
PRECALCULER
ET STOCKER
U=⌊b 2n+1/M⌋
30
ESTIMER QUOTIENT q
=⌊(⌊X/b n⌋·U)/b n+2⌋
32
34
GENERER ERREUR
ALEATOIRE E
RANDOMISER
QUOTIENT
q'=q-1-E
36
RESTER PRES
DU QUOTIENT
q'=q
44
CALCULER
RESTE
R'=X-q'· M
38
CALCULER PRES
DU RESTE
R'=X-q' ·M
46
MULTIPLIER OU
AJOUTER R' A
UN AUTRE RESTE
48
TANT QUE (M≤R')
R':=R'-M
40
R=R'
42
RETOUR

Fig._2

reçue le 12/12/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	35175/FR
N° D'ENREGISTREMENT NATIONAL	0313507

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

METHODE DE REDUCTION MODULAIRE ALEATOIRE ET EQUIPEMENT ASSOCIE

LE(S) DEMANDEUR(S) :

Atmel Corporation
2325 Orchard Parkway
US-SAN JOSE California 95131
U.S.A.

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		DUPAQUIS
Prénoms		Vincent
Adresse	Rue	22 résidence Victor Savine
	Code postal et ville	13120 BIVER
Société d'appartenance *(facultatif)*		
2 Nom		DOUGUET
Prénoms		Michel
Adresse	Rue	594 avenue du Prado Résidence Le Nérée Bât. F
	Code postal et ville	13008 MARSEILLE
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Le 18/11/2003

BRESSE Pierre 92-1038

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.